1. **Резюме по статье «Breaking RSA may not be equivalent to factoring»**

В статье дается опровержение утверждению, что взлом LE-RSA (RSA с низким показателем) эквивалентен факторизации. В статье приводятся доказательства тому, что нарушение алгоритма на самом деле может быть гораздо проще.

В исследовании используются прямолинейные программы (SLP) для многочленов. SLP для многочлена представляет собой последовательность многочленов такая что и для всех значение многочлена ивляется известной величиной и равно либо равен 1, либо переменной или , где и .

Далее определяется понятие прямолинейного сокращения RSA-SLP – алгебраическая схема, в которой элементы выполняют арифметические операции, а также извлекают корни e.

Прямолинейное сокращение – это рандомизированный алгоритм A, который на входе получает n, а на выходе набор RSA-SLP . Для не пренебрежимо-малой части описанный набор должен соответствовать N (с вероятностью, как минимум над случайными битами A).